FIG. 1

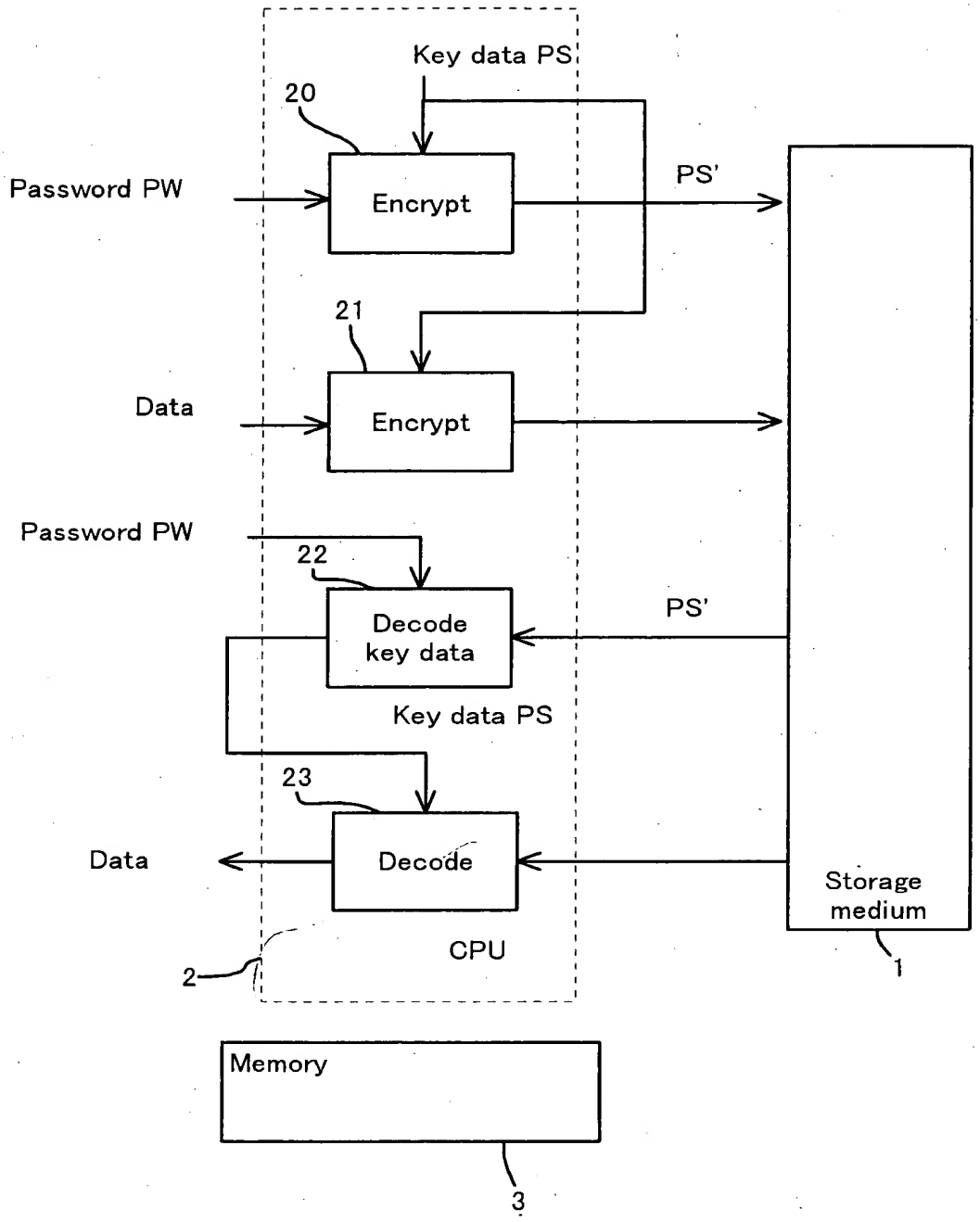

Key data PS
20
Password PW
Encrypt
PS'
21
Data
Encrypt
Password PW
22
Decode
key data
PS'
Key data PS
23
Data
Decode
Storage
medium
CPU
2
1
Memory
3

FIG. 2

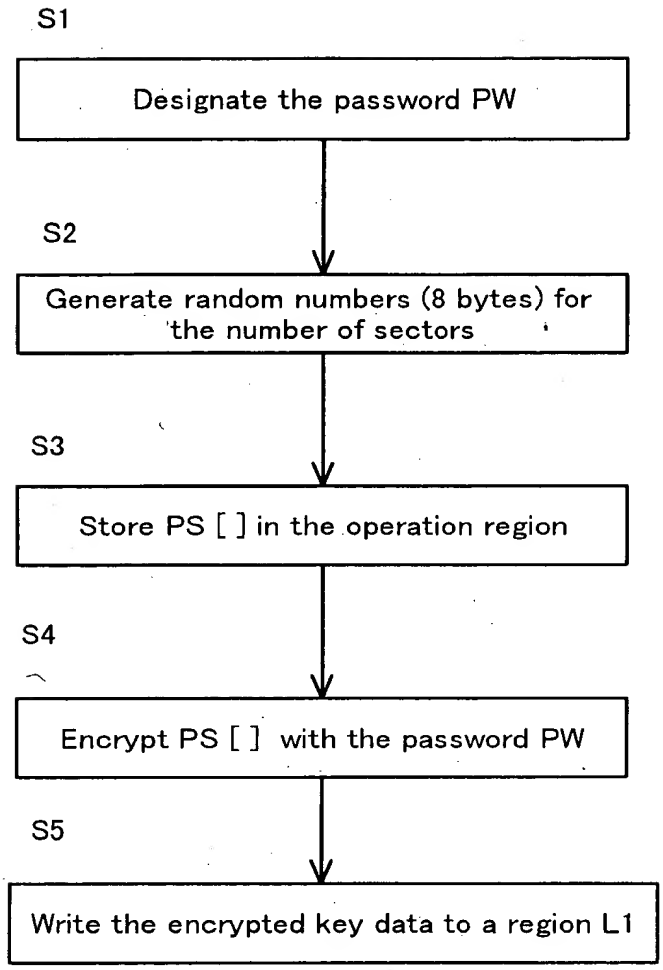
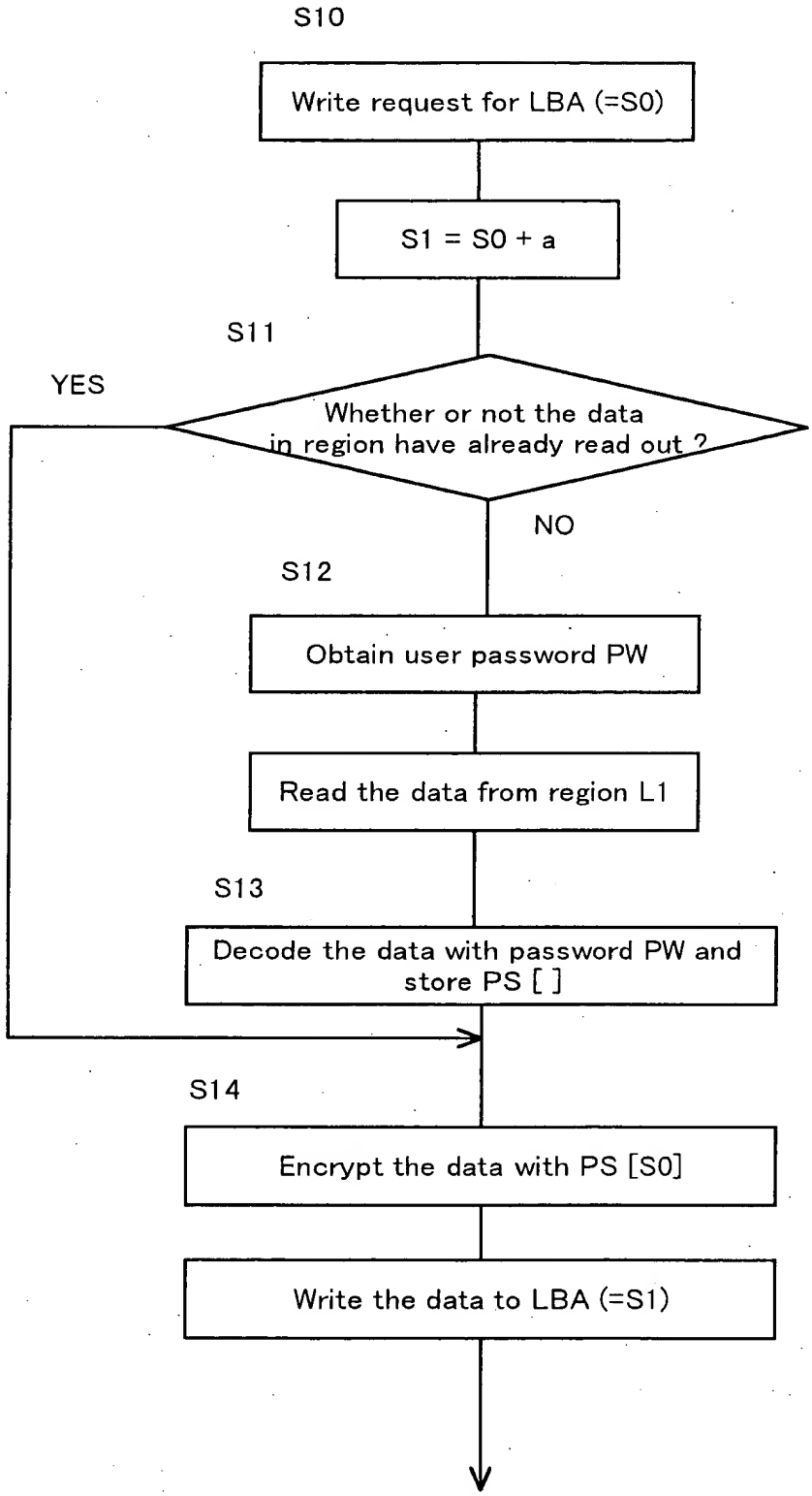

S1
Designate the password PW
S2
Generate random numbers (8 bytes) for the number of sectors
S3
Store PS [ ] in the operation region
S4
Encrypt PS [ ] with the password PW
S5
Write the encrypted key data to a region L1

FIG. 3



8650747 08/29/2006

FIG. 4

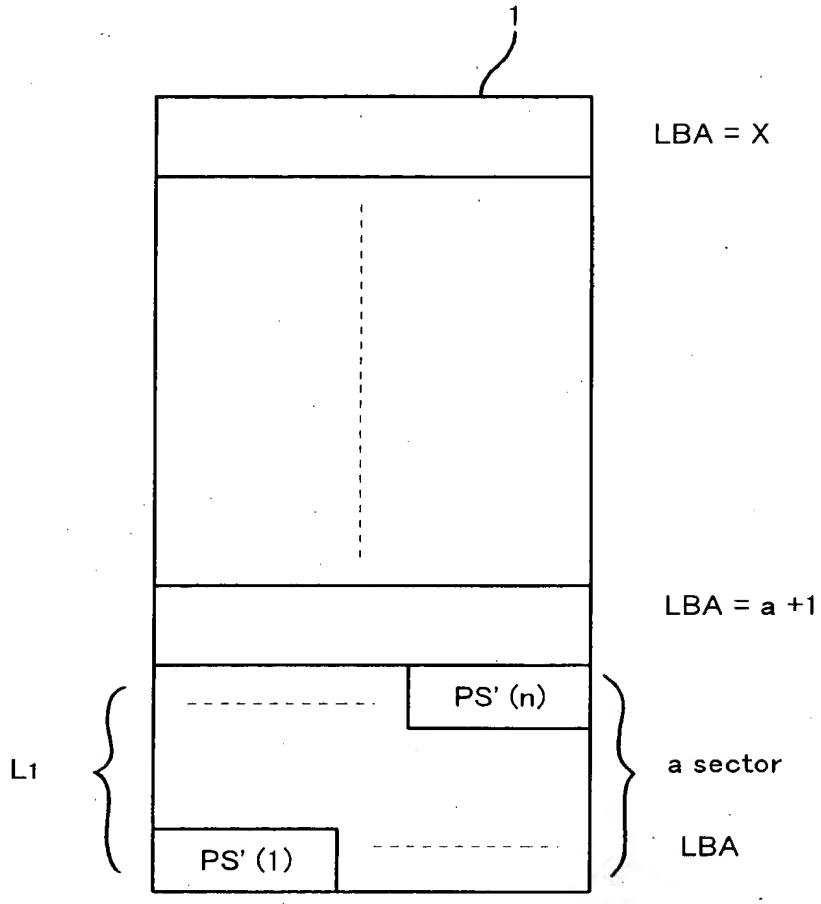
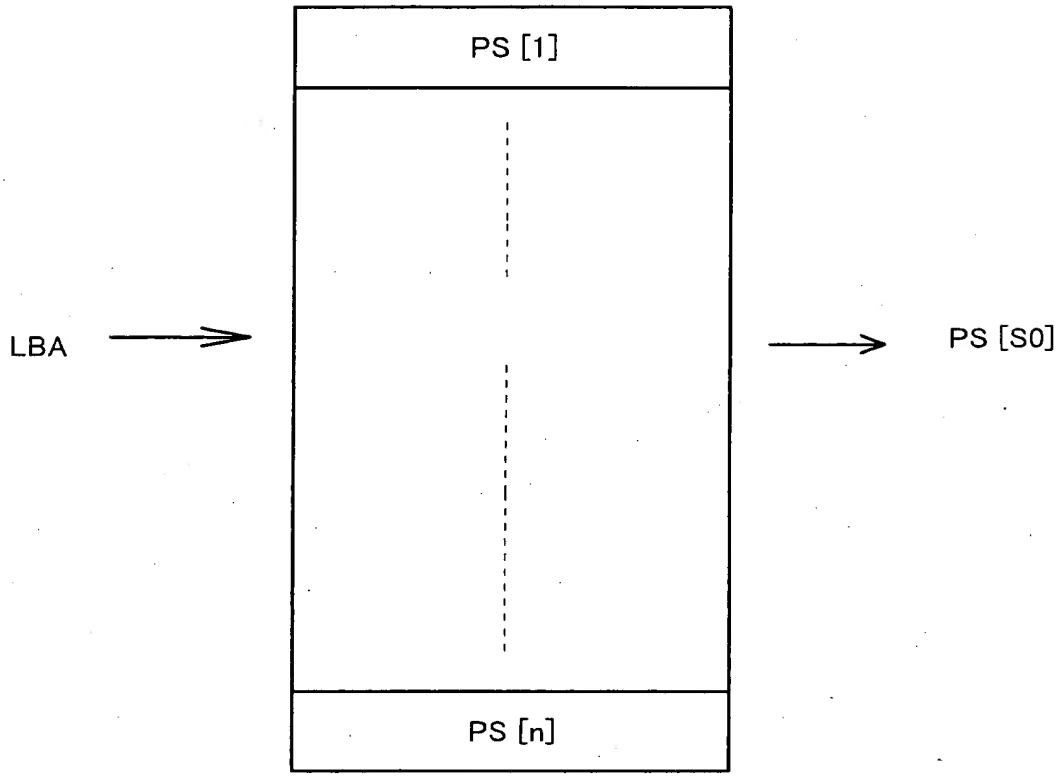


FIG. 5



8659077 "00429160

FIG. 6

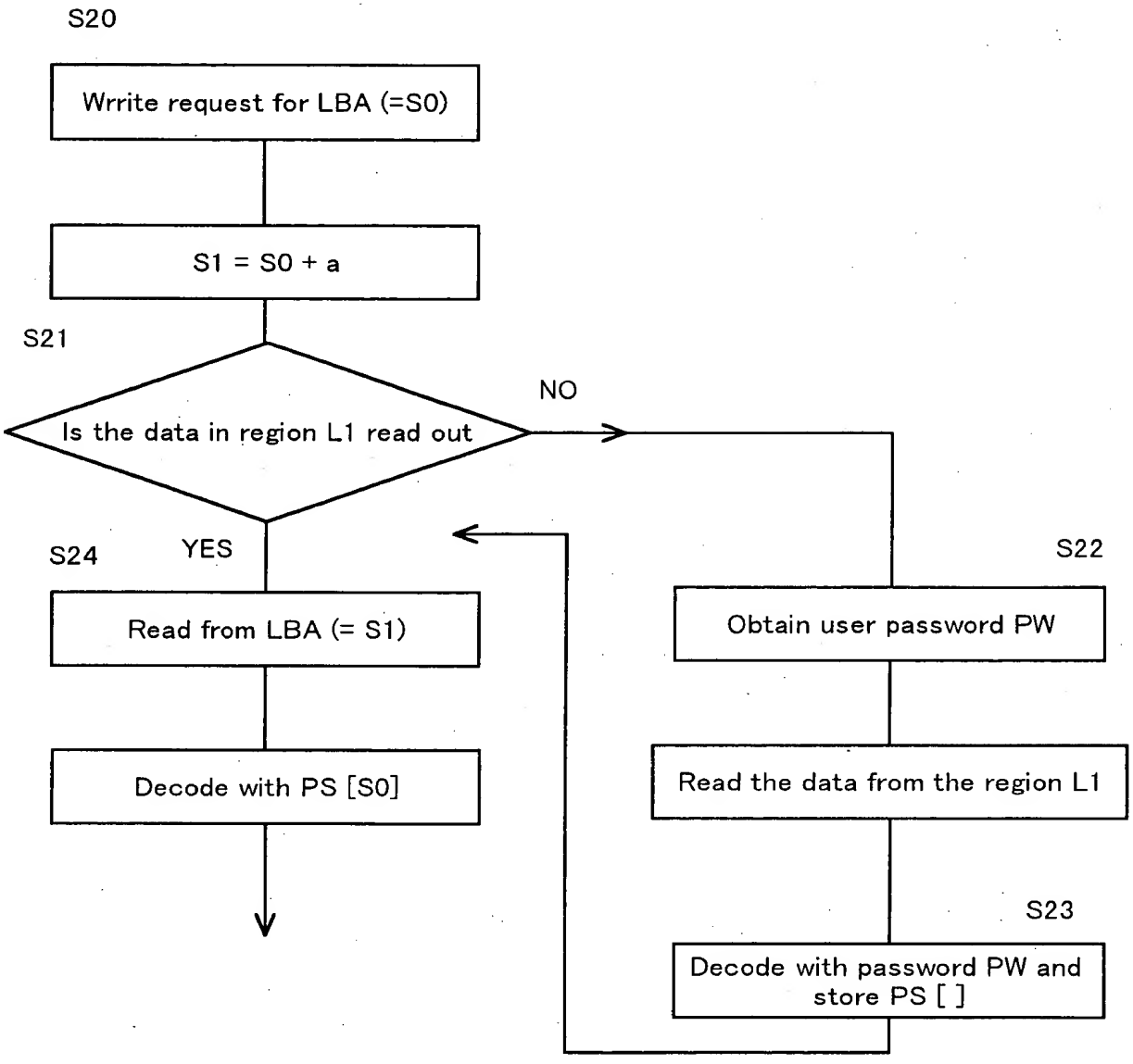

S20
Wrrite request for LBA (=S0)
S1 = S0 + a
S21
Is the data in region L1 read out
NO
YES
S24
Read from LBA (= S1)
Decode with PS [S0]
S22
Obtain user password PW
Read the data from the region L1
S23
Decode with password PW and store PS [ ]

FIG. 7

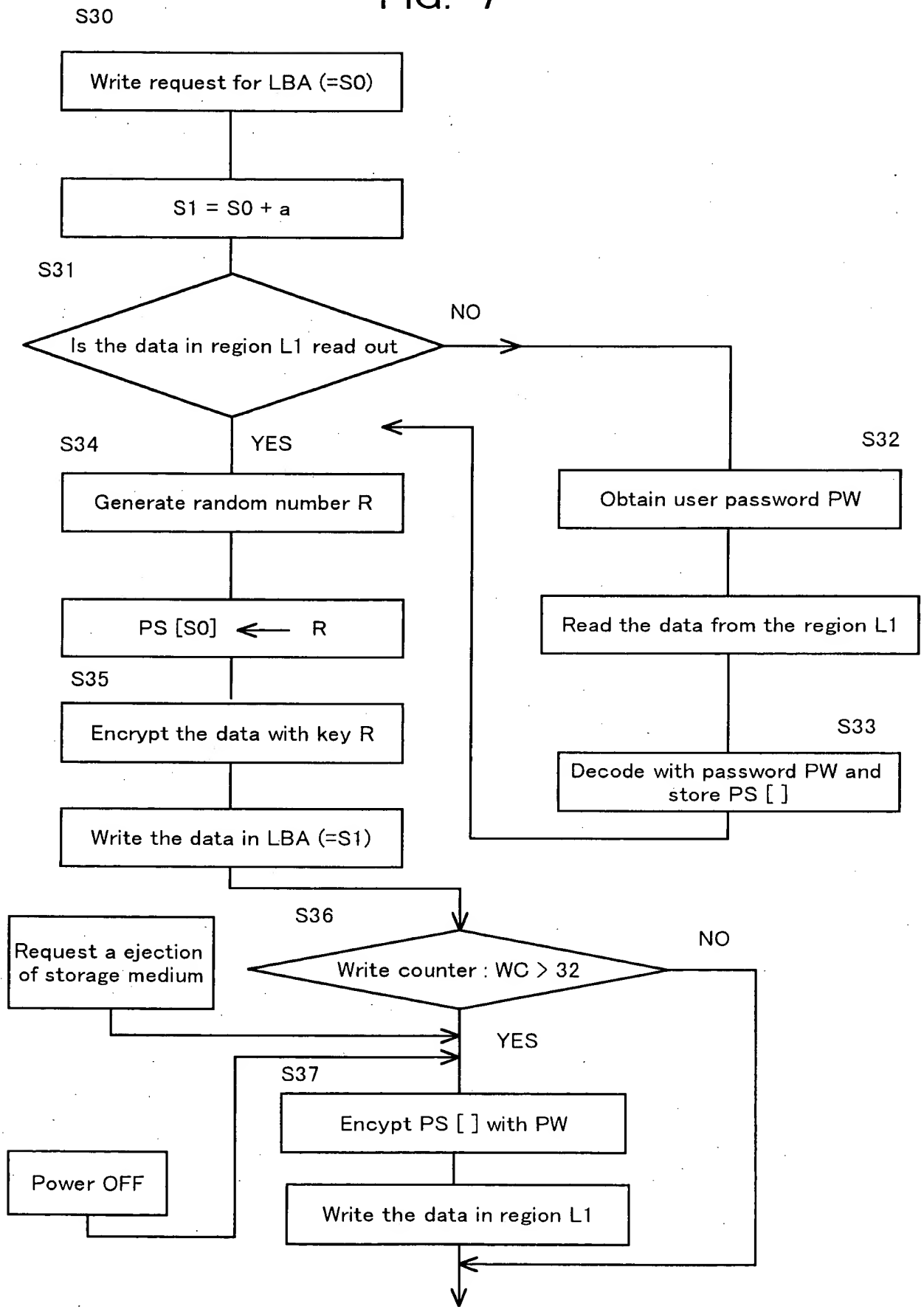

S30
Write request for LBA (=S0)
S1 = S0 + a
S31
Is the data in region L1 read out
NO
YES
S34
Generate random number R
PS [S0] ← R
S35
Encrypt the data with key R
Write the data in LBA (=S1)
S32
Obtain user password PW
Read the data from the region L1
S33
Decode with password PW and store PS [ ]
S36
Write counter : WC > 32
NO
YES
Request a ejection of storage medium
S37
Encypt PS [ ] with PW
Write the data in region L1
Power OFF

FIG. 8

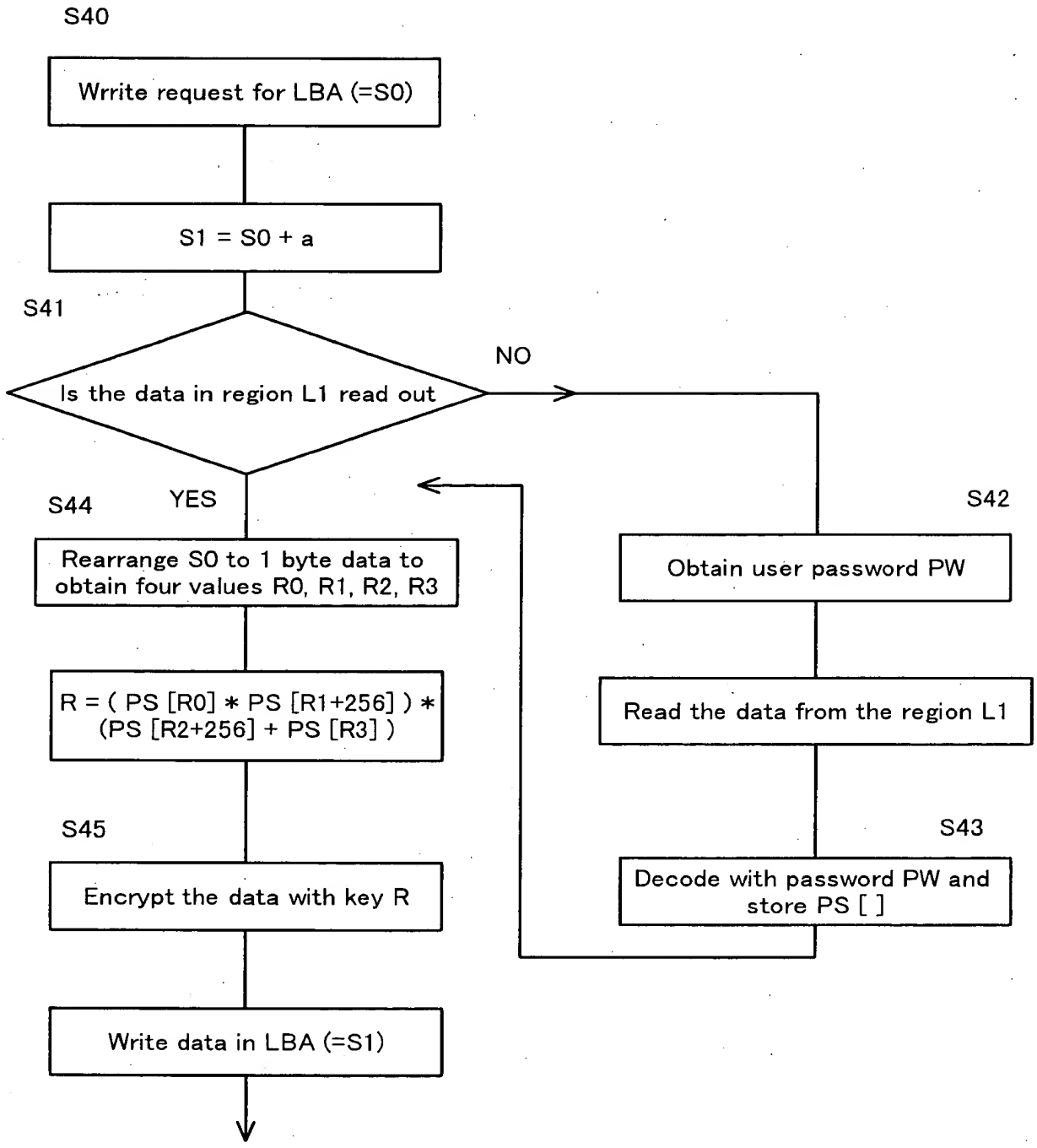
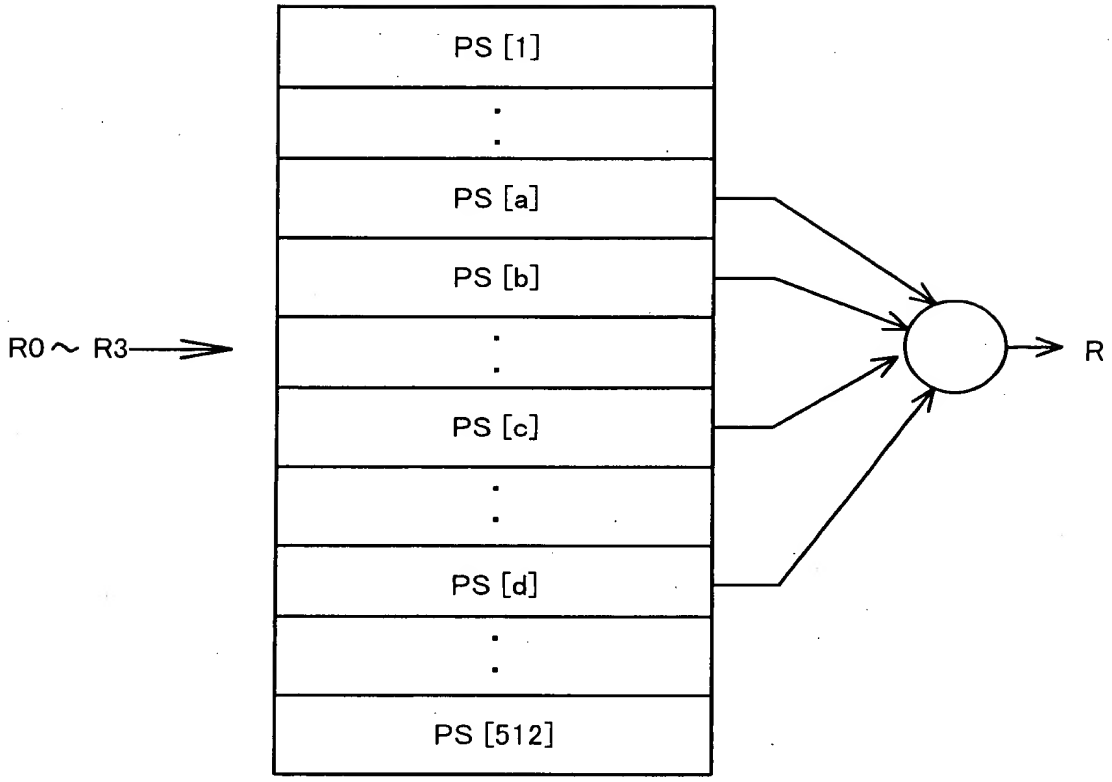

S40
Wrrite request for LBA (=S0)
S1 = S0 + a
S41
Is the data in region L1 read out
NO
YES
S44
Rearrange S0 to 1 byte data to obtain four values R0, R1, R2, R3
R = (PS [R0] * PS [R1+256]) * (PS [R2+256] + PS [R3])
S45
Encrypt the data with key R
Write data in LBA (=S1)
S42
Obtain user password PW
Read the data from the region L1
S43
Decode with password PW and store PS [ ]

FIG. 9



09907,8760 - 0907 - 1409

FIG. 10

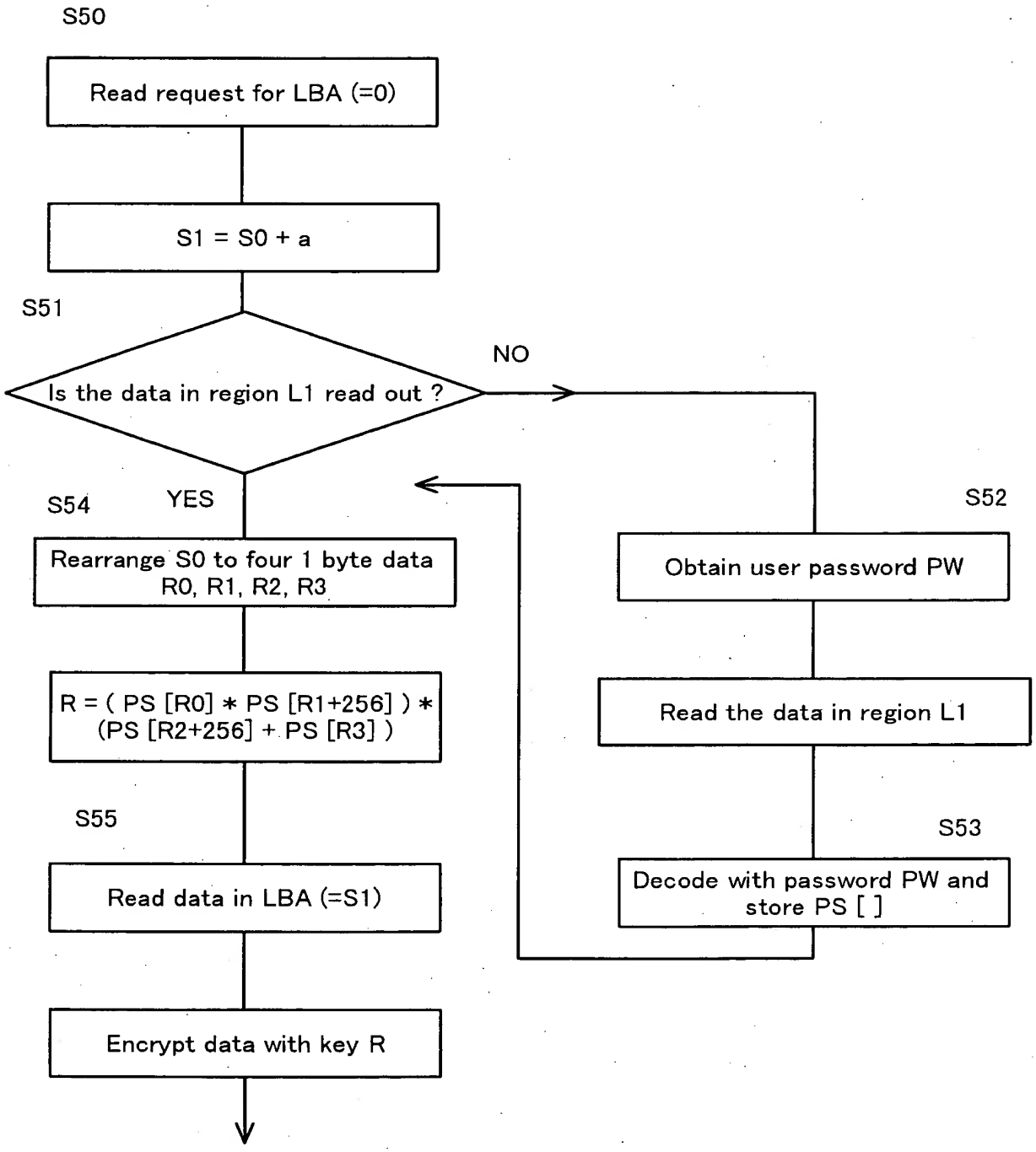

S50
Read request for LBA (=0)
S1 = S0 + a
S51
Is the data in region L1 read out ?
NO
YES
S54
Rearrange S0 to four 1 byte data R0, R1, R2, R3
R = (PS [R0] * PS [R1+256]) * (PS [R2+256] + PS [R3])
S55
Read data in LBA (=S1)
Encrypt data with key R
S52
Obtain user password PW
Read the data in region L1
S53
Decode with password PW and store PS [ ]

FIG. 11

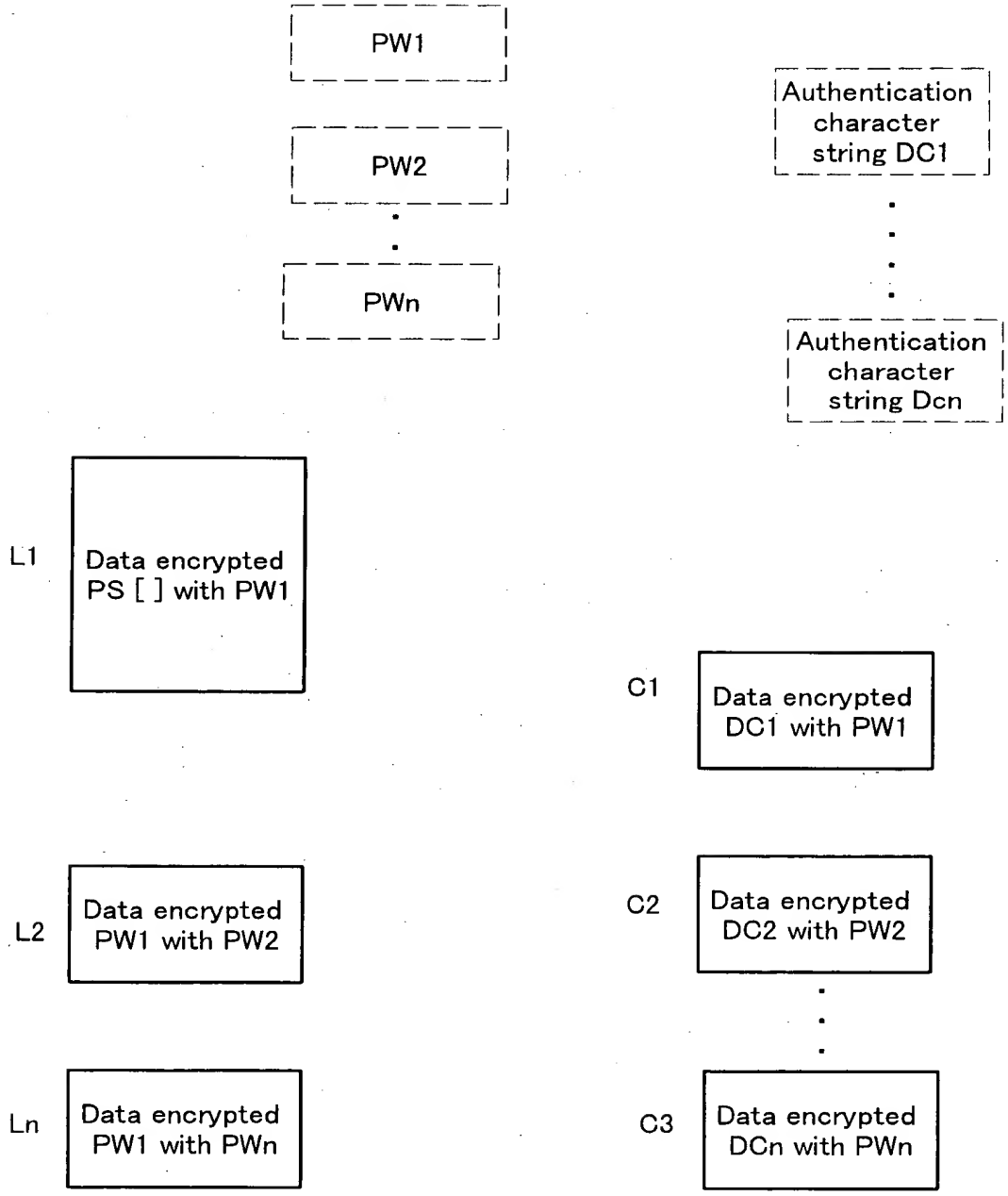
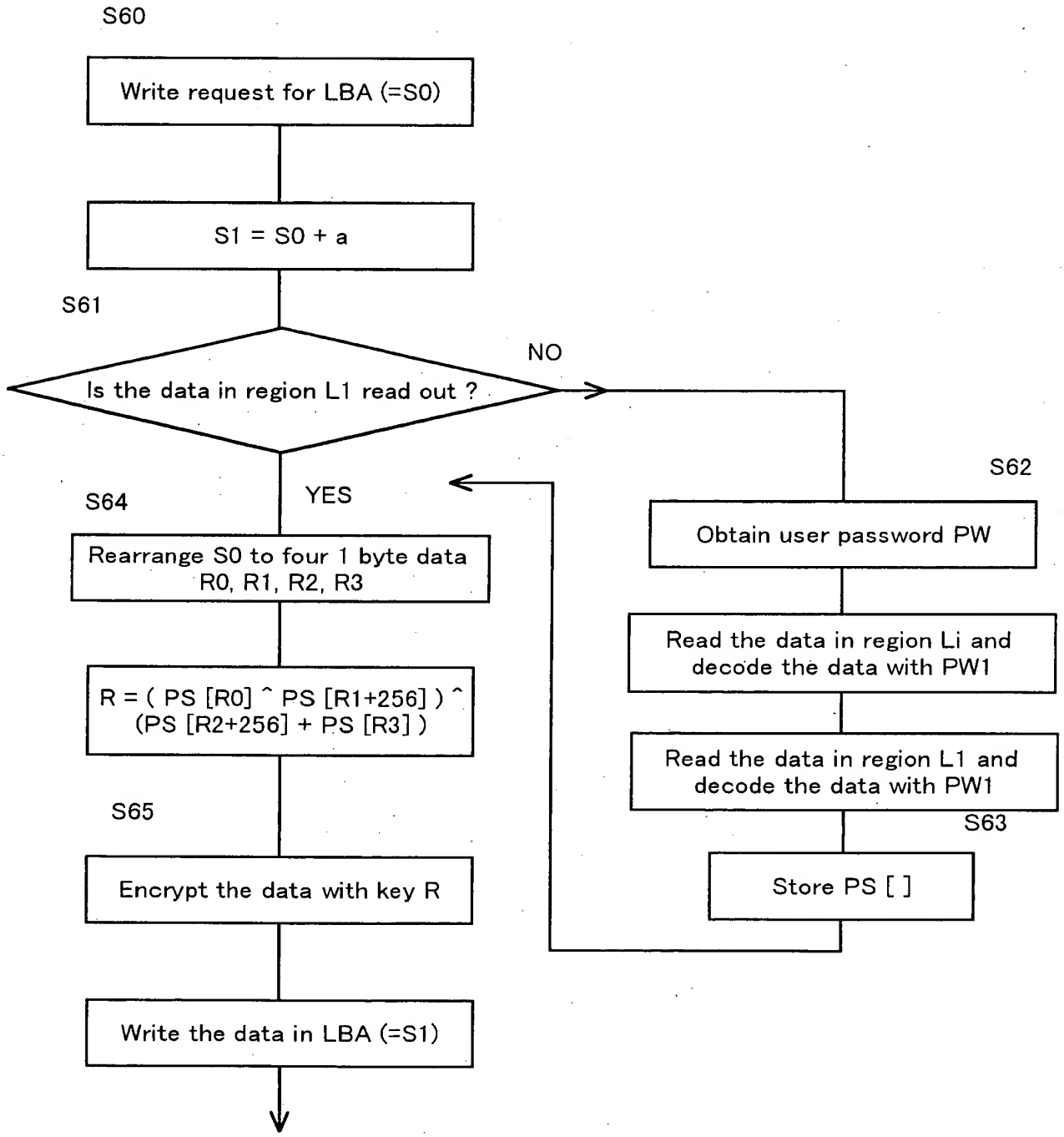
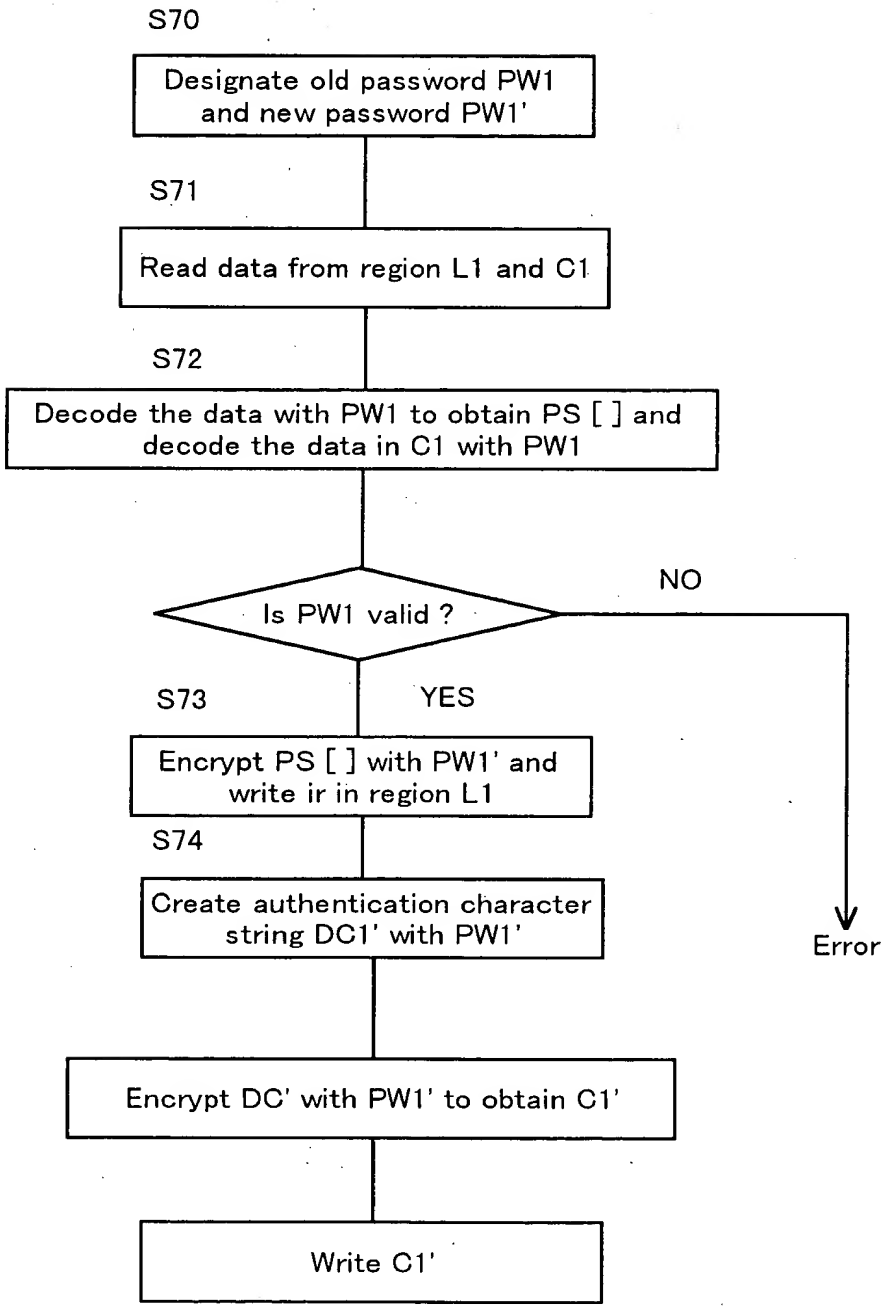

PW1
PW2
PWn
Authentication character string DC1
Authentication character string Dcn
L1
Data encrypted PS [ ] with PW1
L2
Data encrypted PW1 with PW2
Ln
Data encrypted PW1 with PWn
C1
Data encrypted DC1 with PW1
C2
Data encrypted DC2 with PW2
C3
Data encrypted DCn with PWn

FIG. 12



US 2009/0196419 A1

FIG. 13



EP 0 964 398 A2

FIG. 14

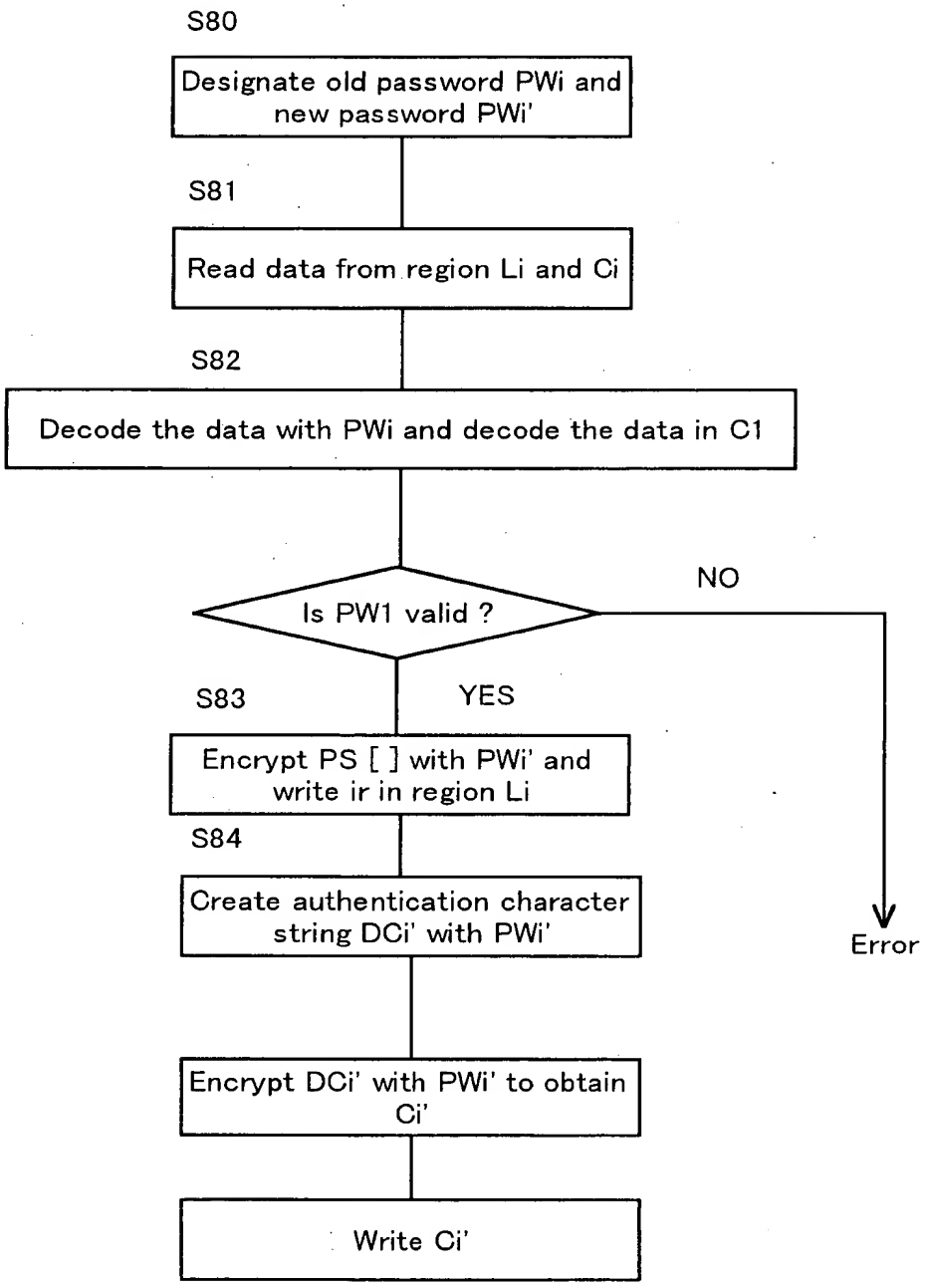
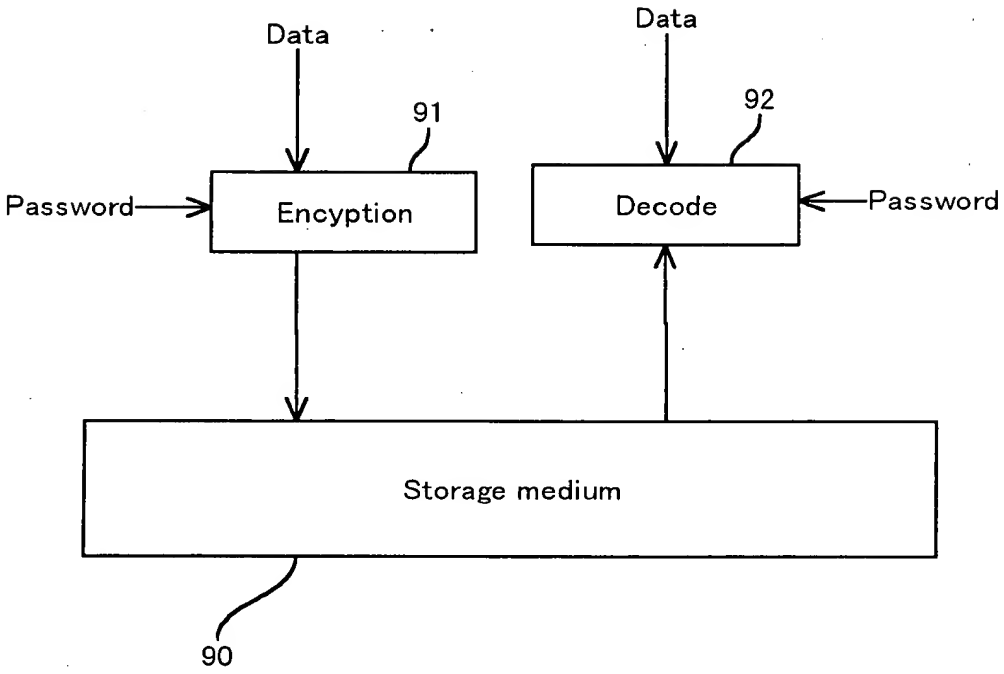

S80
Designate old password PWi and new password PWi'
S81
Read data from region Li and Ci
S82
Decode the data with PWi and decode the data in C1
Is PW1 valid ?
NO
Error
S83
YES
Encrypt PS [ ] with PWi' and write ir in region Li
S84
Create authentication character string DCi' with PWi'
Encrypt DCi' with PWi' to obtain Ci'
Write Ci'

FIG. 15

PRIOR ART